REMARKS[1]

Claims 1, 3-38, and 40-81 remain pending in this application, with claims 1 and

38 being independent.

In the final Office Action, the Examiner made the following claim rejections, all

under 35 U.S.C. § 103(a):

     I.   rejection of claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, 62, and 74-81 as unpatentable over Murphy et al. (U.S. Patent No. 6,226,744) in view of Ishibashi et al. (U.S. Patent Publication No. 2004/0006695);

     II.   rejection of claims 6, 9, 18, 22, 23, 43, 51, 55, 59, 60, and 66 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of de Jong et al. (U.S. Patent No. 7,085,840);

     III.   rejection of claims 7, 8, 44, and 45 as unpatentable over Murphy et al. in view of Ishibashi et al. and de Jong et al., and in further view of Chang et al. (U.S. Patent No. 6,715,082) and Yu et al. (U.S. Patent No. 6,067,621);

     IV.   rejection of claims 19, 24, 26, 56, and 61 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of Teicher et al. (U.S. Patent No. 6,257,486);

     V.   rejection of claims 25, 36, 37, 72, and 73 as unpatentable over Murphy et al. in view of Ishibashi et al., and further in view of Geer, Jr. et al. (U.S. Patent No. 6,192,131);

     VI.   rejection of claims 28-31, 34, 63-65, 67, and 68 as unpatentable over Murphy et al. in view of Ishibashi et al., de Jong et al., Chang et al., and Yu et al., and further in view of Baird, III et al. (U.S. Patent No. 6.732,278); and

     VII.   rejection of claims 32, 33, 35, and 69-71 as unpatentable over Murphy et al. in view of Ishibashi et al., de Jong et al., Chang et al., Yu et al., and Baird, III et al., and further in view of Teppler (U.S. Patent No. 6,792,536).

Applicant respectfully traverses these rejections, as discussed in detail below.

---

[1] The final Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the final Office Action.

I.   **REJECTION OF CLAIMS 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, 62, AND 74-81 UNDER § 103(a)**

Applicant respectfully traverses the rejection of claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, and 62 under 35 U.S.C. § 103(a) as unpatentable over Murphy et al. in view of Ishibashi et al., because a prima facie case of obviousness has not been established. The Examiner has the initial burden of factually supporting any prima facie conclusion of obviousness. See M.P.E.P. § 2142, 8th Ed., Rev. 6 (Sept. 2007). To do so, the Examiner must first establish Graham factual findings, and then make a determination whether the claimed invention "as a whole" would have been obvious to a person of ordinary skill in the art at the time of the invention. Id.; see also M.P.E.P. § 2141.IV. The Graham inquiries include determining the scope and content of the prior art; ascertaining the differences between the claimed invention and the prior art; and resolving the level of ordinary skill in the pertinent art. See M.P.E.P. § 2141.II. The determination of whether the claimed invention would have been obvious based on the factual findings under Graham must be supported with articulated rationales. See M.P.E.P. § 2142 ("The key to supporting any rejection under 35 U.S.C. § 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious."); see also M.P.E.P. § 2143 (providing examples of rationales for supporting an obviousness rejection).

In this case, the rejection of claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 58, and 62 under 35 U.S.C. § 103(a) is improper because the Examiner erred in at least the factual findings, particularly in determining the scope and content of the prior art.

For example, independent claim 1 recites a personal authentication device (PAD) comprising

at least one storage medium storing at least one CA public key, each public key associated with a certificate authority (CA);

one or more input means for receiving one or more digital certificates, wherein the one or more digital certificates comprise at least one ticket-generation certificate including at least one service key generating program or information indicating at least one service key generating program;

a processing component for

authenticating the one or more received digital certificates using the at least one stored CA public key, and

generating at least one service key based on the one or more authenticated digital certificates; and

an output means for outputting the at least one service key.

Neither Murphy et al. nor Ishibashi et al. teaches or suggests a PAD comprising "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key."

Murphy et al. teaches a method and apparatus for authenticating a user over a network, with the network having a client computer and a server computer, and the client computer having a smart card and a smart card reader. See Murphy et al., Abstract.

The Examiner considered the smart card as corresponding to Applicant's claimed PAD. Final Office Action, page 3. However, Murphy et al. fails to teach that the smart card comprises "at least one storage medium storing at least one CA public key." According to Murphy et al., the smart card stores "user information provided by the CA,

such as tokens, digital signatures, certificates, tickets, PIN, human resources

identification number, and so forth, or personal information provided by the user such as

a social security number, birth date, mother's maiden name, etc." Murphy et al., col. 5,

ll. 55-60. Further, the smart card "will generate and store public and private RSA

cryptographic key pairs." Murphy et al., col. 5, ll. 60-63. However, Murphy et al. does

not teach or suggest storing a CA public key in the smart card.

Moreover, the smart card taught by Murphy et al. does not authenticate one or

more digital certification. Rather, "[a] [s]ecure gateway server 18 initiates authentication

of the user of smart card 10 using authentication module 32." Murphy et al., col. 6, ll. 8-

11. The authentication module 32 reads user information from smart card 10, retrieves

authentication information from a database 26, and compares the two sets of

information for authentication of the user of the smart card. See Murphy et al., col. 6, ll.

29-47. Murphy et al. fails to teach or suggest at least that the smart card comprises "a

processing component for authenticating [] one or more received digital certificates

using the at least one stored CA public key," as recited in claim 1.

In summary, Murphy et al. fails to teach or suggest at least a PAD comprising "at

least one storage medium storing at least one CA public key, . . . [and] a processing

component for authenticating [] one or more received digital certificates using the at

least one stored CA public key," as required by independent claim 1.

Ishibashi et al. does not cure the deficiencies of Murphy et al. Ishibashi et al.

describes a system in which child cards are issued based on information stored in a

parent card such that each child card contains only the minimum information. See

Ishibashi et al., paragraph [0013] on page 2. Ishibashi et al. teaches how the parent card and child cards are issued.

In particular, to issue a parent card, a parent-card management authority first downloads a child-card issue application program to an IC card to be issued as the parent card; a registration authority (RA1) and the IC card mutually authenticate each other; the parent-card management authority stores in the parent card a public key, a private key, and a public-key certificate corresponding to the parent card, where the public key and private key are generated by a registration authority (RA1), and the public-key certificate is issued by a certificate authority (CA1). See Ishibashi et al., paragraphs [0157]-[0160] and Fig. 3. The parent card further stores a public-key certificate C(CA1) of CA1. Ishibashi et al., paragraph [0183].

To issue a child card, an IC card to be issued as a child card is first prepared by mutual authentication between a registration authority (RA2) and the IC card, followed by storage in the IC card of a public key and a private key generated by RA2, and a public key certificate issued by a certificate authority CA2. Ishibashi et al., paragraphs [0185]-[0189]. When a user makes a child-card issue request, a reader/writer (R/W) 701 at a child-card issue site reads the parent card and validates the parent card. Ishibashi et al., paragraph [0193]. If the parent card is validated, information such as a private key corresponding to the child card, a public key, a public-key certificate, a public-key certificate of CA2, and an issue certificate, etc., are stored in the child card. Ishibashi et al., paragraphs [0211]-[0212].

Ishibashi et al. apparently describes two verification processes: mutual authentication between an IC card and a registration authority and validation of the

parent card. The mutual authentication process is described in paragraphs

[0161]-[0164] and shown in Fig. 4. The validation of the parent card is described in

paragraphs [0194]-[0205] and shown in Figs. 8 and 9. The mutual authentication

process mutually authenticates the IC card and the registration authority, but does **not**

authenticate one or more digital certificates. See Ishibashi et al., paragraphs

[0161]-[0164] and shown in Fig. 4. The validation of the parent card validates the

public-key certificate stored on the parent card. See Ishibashi et al., paragraphs

[0194]-[0205] and Figs. 8 and 9. However, the validation process is NOT carried out

using "at least one CA public key" stored on at least one storage medium. See

Ishibashi et al., paragraph [0205] (merely teaching that "[a] signature reviewer knows

the public keys").

Therefore, Ishibashi et al. fails to teach or suggest at least a PAD comprising "at

least one storage medium storing at least one CA public key, . . . [and] a processing

component for authenticating [] one or more received digital certificates using the at

least one stored CA public key," as required by independent claim 1.

In summary, neither Murphy et al. nor Ishibashi et al. teaches or suggests "at

least one storage medium storing at least one CA public key, . . . [and] a processing

component for authenticating [] one or more received digital certificates using the at

least one stored CA public key," as required by independent claim 1. The Examiner

failed to recognize such deficiencies of Murphy et al. and Ishibashi et al. with regard to

claim 1. Therefore, the Examiner has not clearly articulated a reason why claim 1 would

be obvious to one of ordinary skill in the art in view of the cited references, and a prima

facie case of obviousness has not been established. The rejection of claim 1 should be

withdrawn.

Independent claim 38 recites, inter alia,

storing on a personal authentication device (PAD) at least one CA
public key, each public key associated with a certificate authority (CA);

. . .

authenticating the one or more received digital certificates using the
at least one stored CA public key.

For reasons similar to those stated above regarding claim 1, neither Murphy et al. nor

Ishibashi et al. teaches or suggests the above-quoted elements of claim 38. The

Examiner failed to recognize such deficiencies of Murphy et al. and Ishibashi et al. with

regard to claim 38. Therefore, the Examiner has not clearly articulated a reason why

claim 38 would be obvious to one of ordinary skill in the art in view of the cited

references, and a prima facie case of obviousness has not been established. The

rejection of claim 38 should be withdrawn.

Claims 2-5, 10-13, 15-17, 20, 21, 27, 39-42, 46-50, 52-54, 57, 58, 62, and 74-81

respectively depend from claims 1 and 38 and therefore respectively incorporate all

elements of claims 1 and 38. For the same reasons stated above with regard to claims

1 and 38, the rejection of claims 2-5, 10-13, 15-17, 20, 21, 27, 39-42, 46-50, 52-54, 57,

58, 62, and 74-81 is improper and should be withdrawn.

II.   REJECTION OF CLAIMS 6, 9, 18, 22, 23, 43, 51, 55, 59, 60, AND 66 UNDER § 103(a)

Applicant respectfully traverses the rejection of claims 6, 9, 18, 22-23, 43, 51, 55,

59, 60, and 66 under 35 U.S.C. § 103(a) as being unpatentable over Murphy et al. in

view of Ishibashi et al., and further in view of de Jong et al.

As discussed above, neither <u>Murphy et al.</u> nor <u>Ishibashi et al.</u> teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to <u>de Jong et al.</u> are correct, which Applicant does not concede, <u>de Jong et al.</u> also does not teach or suggest the quoted elements of claims 1 and 38.

Claims 6, 9, 18, 22-23, 43, 51, 55, 59, 60, and 66 respectively depend from claims 1 and 38, and respectively incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of <u>Murphy et al.</u>, <u>Ishibashi et al.</u>, and <u>de Jong et al.</u> with respect to claims 1 and 38. Therefore, the Examiner has not clearly articulated a reason why claims 6, 9, 18, 22-23, 43, 51, 55, 59, 60, and 66 would be obvious to one of ordinary skill in the art in view of the cited references, and a <u>prima facie</u> case of obviousness has not been established. The rejection of claims 6, 9, 18, 22-23, 43, 51, 55, 59, 60, and 66 should be withdrawn.

III.   <u>REJECTION OF CLAIMS 7, 8, 44, AND 45 UNDER § 103(a)</u>

Applicant respectfully traverses the rejection of claims 7, 8, 44, and 45 under 35 U.S.C. § 103(a) as being unpatentable over <u>Murphy et al.</u> in view of <u>Ishibashi et al.</u> and <u>de Jong et al.</u>, and in further view of <u>Chang et al.</u> and <u>Ye</u>.

As discussed above, neither <u>Murphy et al.</u> nor <u>Ishibashi et al.</u> nor <u>de Jong et al.</u> teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to <u>Chang et al.</u> and <u>Yu et al.</u> are correct, which Applicant does not concede, neither <u>Chang et al.</u> nor <u>Yu et al.</u> teaches or suggests the quoted elements of claims 1 and 38.

Claims 7, 8, 44, and 45 respectively depend from claims 1 and 38, and respectively incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of <u>Murphy et al.</u>, <u>Ishibashi et al.</u>, <u>de Jong et al.</u>, <u>Chang et al.</u>, and <u>Yu et al.</u> with respect to claims 1 and 38. Therefore, the Examiner has not clearly articulated a reason why claims 7, 8, 44, and 45 would be obvious to one of ordinary skill in the art in view of the cited references, and a <u>prima facie</u> case of obviousness has not been established. The rejection of claims 7, 8, 44, and 45 should be withdrawn.

IV. <u>REJECTION OF CLAIMS 19, 24, 26, 56, AND 61 UNDER § 103(a)</u>

Applicant respectfully traverses the rejection of claims 19, 24, 26, 56, and 61 under 35 U.S.C. § 103(a) as being unpatentable over <u>Murphy et al.</u> in view of <u>Ishibashi et al.</u>, and further in view of <u>Teicher et al.</u>.

As discussed above, neither <u>Murphy et al.</u> nor <u>Ishibashi et al.</u> teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to <u>Teicher et al.</u> are correct, which Applicant does not concede, <u>Teicher et al.</u> does not teach or suggest the quoted elements of claims 1 and 38.

Claims 19, 24, 26, 56, and 61 depend from claims 1 and 38, and incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of <u>Murphy et al.</u>, <u>Ishibashi et al.</u>, and <u>Teicher et al.</u> with respect to claims 1 and 38. Therefore, the Examiner has not clearly articulated a reason why claims 19, 24, 26, 56, and 61 would be obvious to one of ordinary skill in the art in view of the cited references, and a <u>prima facie</u> case of obviousness has not been established. The rejection of claims 19, 24, 26, 56, and 61 should be withdrawn.

V.   **REJECTION OF CLAIMS 25, 36, 37, 72, AND 73 UNDER § 103(a)**

Applicant respectfully traverses the rejection of claims 25, 36, 37, 72, and 73 under 35 U.S.C. § 103(a) as being unpatentable over <u>Murphy et al.</u> in view of <u>Ishibashi et al.</u> and <u>Geer, Jr. et al.</u>

As discussed above, neither <u>Murphy et al.</u> nor <u>Ishibashi et al.</u> teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a

processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key," as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to Geer, Jr. et al. are correct, which Applicant does not concede, Geer, Jr. et al. does not teach or suggest the quoted elements of claims 1 and 38.

Claims 25, 36, 37, 72, and 73 depend from claims 1 and 38, and incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of Murphy et al., Ishibashi et al., and Geer, Jr. et al. with respect to claims 1 and 38. Therefore, the Examiner has not clearly articulated a reason why claims 25, 36, 37, 72, and 73 would be obvious to one of ordinary skill in the art in view of the cited references, and a prima facie case of obviousness has not been established. The rejection of claims 25, 36, 37, 72, and 73 should be withdrawn.

VI.   REJECTION OF CLAIMS 28-31, 34, 63-65, 67, AND 68 UNDER § 103(a)

Applicant respectfully traverses the rejection of claims 28-31, 34, 63-65, 67, and 68 under 35 U.S.C. § 103(a) as being unpatentable over Murphy et al. in view of Ishibashi et al. and de Jong et al., and in further view of Chang et al., Yu et al., and Baird, III et al.

As discussed above, neither Murphy et al., nor Ishibashi et al., nor de Jong et al., nor Chang et al., nor Yu et al. teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one

or more received digital certificates using the at least one stored CA public key," as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to Baird, III et al. are correct, which Applicant does not concede, Baird, III et al. does not teach or suggest the quoted elements of claims 1 and 38.

Claims 28-31, 34, 63-65, 67, and 68 respectively depend from claims 1 and 38, and respectively incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of Murphy et al., Ishibashi et al., de Jong et al., and Chang et al., Yu et al., and Baird, III et al. with respect to claims 1 and 38. Therefore, the Examiner has not clearly articulated a reason why claims 28-31, 34, 63-65, 67, and 68 would be obvious to one of ordinary skill in the art in view of the cited references, and a prima facie case of obviousness has not been established. The rejection of claims 28-31, 34, 63-65, 67, and 68 should be withdrawn.

VII. REJECTION OF CLAIMS 32, 33, 35, AND 69-71 UNDER § 103(a)

Applicant respectfully traverses the rejection of claims 32, 33, 35, and 69-71 under 35 U.S.C. § 103(a) as being unpatentable over Murphy et al. in view of Ishibashi et al., de Jong et al., and in further view of Yu et al., Baird, III et al., and Teppler.

As discussed above, neither Murphy et al., nor Ishibashi et al., nor de Jong et al., nor nor Yu et al., nor Baird, III et al. teaches or suggests "at least one storage medium storing at least one CA public key, . . . [and] a processing component for authenticating [] one or more received digital certificates using the at least one stored CA public key,"

13

as required by independent claims 1, or the steps of "storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); . . . authenticating the one or more received digital certificates using the at least one stored CA public key," as recited in claim 38. Even if the Examiner's allegations with respect to Teppler are correct, which Applicant does not concede, Teppler does not teach or suggest the quoted elements of claims 1 and 38.

Claims 32, 33, 35, and 69-71 respectively depend from claims 1 and 38, and respectively incorporate all elements of claims 1 and 38. The Examiner failed to recognize the above-noted deficiencies of Murphy et al., Ishibashi et al., de Jong et al., Yu et al., Baird, III et al., and Teppler. Therefore, the Examiner has not clearly articulated a reason why claims 32, 33, 35, and 69-71 would be obvious to one of ordinary skill in the art in view of the cited references, and a prima facie case of obviousness has not been established. The rejection of claims 32, 33, 35, and 69-71 should be withdrawn.

In view of the foregoing remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 5, 2007   By:_____
                                        Qingyu Yin
                                        Reg. No. 61,329